7

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077274
(43)Date of publication of application : 15.03.2002

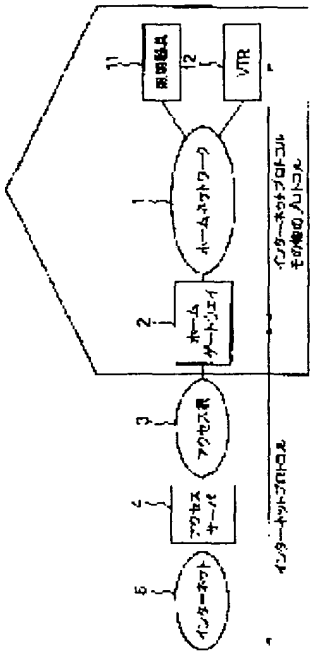
(51)Int.Cl. H04L 12/66
H04L 12/28
H04L 29/06

(21)Application number : 2000-263873
(22)Date of filing : 31.08.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : SAITO TAKESHI

(54) HOME GATEWAY DEVICE, ACCESS SERVER AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communications system, capable of preventing an attack from a hostile user to a home network, without having to provide excessive security functions to a home gateway or requiring a special management of a user.
SOLUTION: In order to access a VTR 12 on a home network 1 via the Internet 5 from a mobile terminal, an access number corresponding to a home gateway 2 is specified, and a message is transmitted to an access server 4; the access server 4 authenticates the mobile terminal by a predetermined method and when the authentication is confirmed, the message is transmitted to the home gateway 2 provided in the home network 1 corresponding to the specified access number via an access network 3; and the home gateway 2 receiving the massage from the access server 4 which has previously been registered transmits the message to the VTR 12 via the home network 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－77274
（P2002－77274A）
(43)公開日　平成14年３月15日(2002.3.15)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/28		11/00	３１０Ｚ	５Ｋ０３３
29/06		13/00	３０５Ｂ	５Ｋ０３４

審査請求　未請求　請求項の数21　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－263873(P2000－263873)

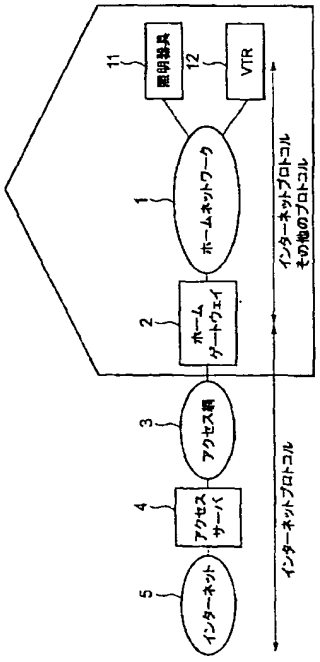
(22)出願日　平成12年８月31日(2000.8.31)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5K030 GA15 HA06 HC01 HC14 HD03
HD06 JA07 JA11 KA04
5K033 AA08 BA01 CB02 CB08 DA01
DA06 DB12 DB16
5K034 AA05 FF01 HH01 HH16 HH17
HH26 HH63

(54)【発明の名称】　ホームゲートウェイ装置、アクセスサーバ装置及び通信方法

(57)【要約】
【課題】　ホームゲートウェイに過度なセキュリティ機能を実装したり、そのユーザに専門的な管理を要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を防ぐことを可能とする通信システムを提供すること。
【解決手段】　携帯端末からインターネット５を介しホームネットワーク１上のＶＴＲ１２にアクセスするためにホームゲートウェイ２に対応するアクセス番号を指定してアクセスサーバ４へメッセージを送信し、アクセスサーバ４は携帯端末との間で該携帯端末について予め定められた方法で認証手続きを行い認証に成功した場合に指定されたアクセス番号に対応するホームネットワーク１に設置されたホームゲートウェイ２へアクセス網３を介してメッセージを転送し、予め登録されたアクセスサーバ４からメッセージを受信したホームゲートウェイ２はホームネットワーク１を介してＶＴＲ１２へメッセージを転送する。



1

【特許請求の範囲】

【請求項１】ホームネットワークの外部に位置する第１の通信装置から該ホームネットワーク上の第２の通信装置にアクセスするために、該第１の通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、

前記所定のメッセージを受信した前記アクセスサーバ装置は、前記第１の通信装置との間で、該第１の通信装置について、予め定められた認証方法に従って認証手続きを行い、

前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、

予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージを、前記第２の通信装置がサポートするプロトコルに変換した上で、該ホームネットワークを介して、前記第２の通信装置へ転送することを特徴とする通信方法。

【請求項２】前記ホームゲートウェイ装置は、前記所定のメッセージを前記第２の通信装置に転送した後に該第２の通信装置から情報を受信した場合には、該情報を、プロトコル変換した上で、前記アクセスサーバ装置を経由して、前記第１の通信装置に転送することを特徴とする請求項１に記載の通信方法。

【請求項３】ホームネットワークの外部に位置する通信装置から該ホームネットワークにアクセスするために、該通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、

前記所定のメッセージを受信した前記アクセスサーバ装置は、前記通信装置との間で、該通信装置について、予め定められた認証方法に従って認証手続きを行い、

前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、

予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージに基づいて選択された該ホームネットワークに関係する情報を含むホームページを、前記アクセスサーバ装置を経由して、前記通信装置に転送することを特徴とする通信方法。

【請求項４】登録されたホームネットワークのホームゲートウェイ装置に対するアクセス制御を行うアクセスサーバ装置であって、

2

自装置がアクセス制御を行う対象とする前記ホームゲートウェイ装置にアクセスするために使用すべき第１のアクセス番号と、該ホームゲートウェイ装置の設置されるホームネットワークの外部に位置する第１の通信装置が該ホームゲートウェイ装置または該ホームネットワーク上の第２の通信装置に所定のメッセージを送信する際に自装置へアクセスするために使用すべき第２のアクセス番号と、自装置が該第１の通信装置との間で行うべき認証方法とを対応付けて登録した認証テーブルを記憶する手段と、

前記ホームネットワークの外部に位置する第１の通信装置から、前記第２のアクセス番号の使用により、前記所定のメッセージを受信する手段と、

使用された前記第２のアクセス番号から前記認証テーブルを参照して得られる認証方法に従って、前記第１の通信装置との間で認証手続きを行う手段と、

前記認証に成功した場合に、使用された前記第２のアクセス番号から前記認証テーブルを参照して得られる前記第１のアクセス番号を使用し、所定のアクセス網を介して、前記ホームゲートウェイ装置へ、前記所定のメッセージを送信する手段とを備えたことを特徴とするアクセスサーバ装置。

【請求項５】前記所定のメッセージを前記ホームゲートウェイ装置に転送した後に該ホームゲートウェイ装置から情報を受信する手段と、

受信した該情報を、前記第１の通信装置に転送するために、前記第１の通信装置へ送信する手段とを更に備えたことを特徴とする請求項４に記載のアクセスサーバ装置。

【請求項６】前記情報は、前記ホームゲートウェイ装置により作成された、該ホームゲートウェイ装置の設置されたホームネットワーク上に接続されている機器に関する内容を含むホームページであることを特徴とする請求項５に記載のアクセスサーバ装置。

【請求項７】前記情報は、前記所定のメッセージを転送した前記第２の通信装置から送信され、該ホームゲートウェイ装置によりプロトコル変換された、所定の形式のデータであることを特徴とする請求項５に記載のアクセスサーバ装置。

【請求項８】前記ホームゲートウェイ装置との間の通信を、暗号処理または改ざん防止処理を施した上で行なうことを特徴とする請求項４のアクセスサーバ装置。

【請求項９】前記認証テーブルに、複数のホームゲートウェイ装置を登録可能としたことを特徴とする請求項４のアクセスサーバ装置。

【請求項１０】前記アクセスサーバ装置は、前記アクセス網を提供する通信事業者によって提供されるものであることを特徴とする請求項４ないし９に記載のアクセスサーバ装置。

【請求項１１】前記第１の通信装置は、インターネット

を介して、前記アクセスサーバ装置へアクセスすることを特徴とする請求項４ないし１０に記載のアクセスサーバ装置。

【請求項１２】前記アクセスサーバ装置へ専用線を介してアクセスすることを特徴とする請求項４ないし１１に記載のアクセスサーバ装置。

【請求項１３】ホームネットワークに接続可能な家電機器に関して制御画面を含むデータを登録したデータベースを記憶する手段と、

前記ホームゲートウェイ装置から未知の家電機器に関する問い合わせメッセージを受信する手段と、

問い合わせを受けた前記家電機器のデータについて前記データベースを検索する手段と、

前記検索の結果得られたデータを含む応答メッセージを、問い合わせもとの前記ホームゲートウェイ装置に送信する手段とを更に備えたことを特徴とする請求項４ないし１２に記載のアクセスサーバ装置。

【請求項１４】前記認証テーブルに登録された前記ホームゲートウェイに対して、該ホームゲートウェイの設置されたホームネットワークから外部への方向のアクセスに対して、プロキシサーバ処理を代行して行うための手段を更に備えたことを特徴とする請求項４ないし１３に記載のアクセスサーバ装置。

【請求項１５】前記ホームゲートウェイ装置は、自装置が設置されたホームネットワークの外部からのアクセスについては、予め登録された前記アクセスサーバ装置からのアクセスのみを許可するものであることを特徴とする請求項４ないし１４に記載のアクセスサーバ装置。

【請求項１６】ホームネットワークに設置されるホームゲートウェイ装置であって、

前記ホームネットワークと所定のアクセス網との間を中継するための手段と、

前記所定のアクセス網を介して通信可能な、自装置に対するアクセス制御を依頼しているアクセスサーバ装置を登録するための手段と、

自装置が設置されたホームネットワークの外部からのアクセスを受けた際に、予め登録された前記アクセスサーバ装置からのアクセスのみを許可する手段とを備えたことを特徴とするホームゲートウェイ装置。

【請求項１７】前記アクセスが許可された場合に、前記アクセスサーバ装置から受信した所定のメッセージを、自装置の接続されたホームネットワークのプロトコルにプロトコル変換した上で、該ホームネットワーク上の宛先通信装置に転送する手段を更に備えたことを特徴とする請求項１６に記載のホームゲートウェイ装置。

【請求項１８】前記宛先通信装置に前記所定のメッセージを転送した後に該宛先通信装置から受信した所定の形式のＡＶデータを、前記アクセスサーバに中継する手段と、

受信した前記所定の形式のＡＶデータに対して所定の変換処理を施す手段とを更に備えたことを特徴とする請求項１７に記載のホームゲートウェイ装置。

【請求項１９】前記アクセスが許可された場合に、前記アクセスサーバ装置から受信した所定のメッセージに応答して、自装置の接続されたホームネットワーク上に接続されている機器に関する内容を含むホームページを返送する手段を更に備えたことを特徴とする請求項１６に記載のホームゲートウェイ装置。

【請求項２０】自装置の設置されたホームネットワークについて自動構成認識を行う手段と、

前記自動構成認識において、前記ホームネットワーク上に、予め登録されていない未知の種類の機器又はサービスが検出された場合に、該未知の機器又はサービスに関する問い合わせメッセージを前記アクセスサーバ装置に送信する手段と、

前記アクセスサーバ装置から、問い合わせた前記未知の機器又はサービスに関するデータを含む応答メッセージを受信する手段とを更に備えたことを特徴とする問い合わせることを特徴とする請求項１６に記載のホームゲートウェイ装置。

【請求項２１】前記アクセスサーバ装置との間の通信を、暗号処理または改ざん防止処理を施した上で行なうことを特徴とする請求項１６ないし２０のいずれか１項に記載のホームゲートウェイ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ホームネットワークに設置されるホームゲートウェイ装置、ホームゲートウェイ装置へのアクセスを制御するアクセスサーバ装置及び通信方法に関する。

【０００２】

【従来の技術】デジタル家電の急速な普及に伴い、家電機器同士をネットワーク接続するいわゆる「ホームネットワーク」が急速に普及しようとしている。これは、ＡＶ機器に代表されるＩＥＥＥ１３９４、白物家電に代表されるエコーネット、パソコンや周辺機器に代表されるイーサネット（登録商標）やＵＳＢ等、分野を問わない現象である。

【０００３】これらのホームネットワークをインターネットと接続し、家電製品にインターネット接続機能を持たせたり、インターネットから家電機器の制御を行なうことを可能としようとする動きが活発である。このために必要な装置が、ホームネットワークと公衆網（インターネット）との間に位置し、ホームネットワークへの入口ノードともいうべき「ホームゲートウェイ」である。ホームゲートウェイは、ホームルータの機能の他、インターネットプロトコルを理解しない機器がホームネットワーク上に多く存在することが考えられることから、プロトコル変換機能（いわゆるゲートウェイ機能）が備わっているのが一般的である。

5

【０００４】このような装置の登場により、インターネットからホームネットワーク上の装置の遠隔制御等が可能になると考えられる。

【０００５】

【発明が解決しようとする課題】この場合、問題になると考えられるのがセキュリティの問題である。すなわち、インターネット上には悪意ユーザ（例えば、特定または不特定の通信機器あるいはネットワークなどに対して不正あるいは違法の通信行為等を働こうとするあるいはその可能性のあるユーザ）が数多く存在することを前提とする必要があり、これらの悪意ユーザからのアタックを想定する必要がある。

【０００６】企業ネットワークの場合には、企業ネットワークの入口ノードに「ファイアウォール」を配置し、ここで悪意ユーザからのアタックをシャットアウトするような方法が一般的であった。ところが、このような方法は、企業ネットワークに「ネットワーク管理者」を担当する者が存在し、該担当者が、セキュリティに関する適切な設定や、日々更新される「パッチあて」の作業等、セキュリティに関する管理業務を行なっていることが、暗黙の了解となっている。

【０００７】これに対して、ホームネットワークの場合には、各一般家庭に、ホームゲートウェイへのセキュリティに関する適切な設定を行なうことのできるネットワーク管理者の存在を要求することはできない。したがって、ホームネットワークでは、ネットワーク管理者の存在を要求できる企業ネットワークのようにファイアウォール等によって悪意ユーザからの攻撃を防ぐというような技術を一般的に用いることはできない。

【０００８】本発明は、上記事情を考慮してなされたもので、ホームゲートウェイに過度なセキュリティ機能を実装したり、ホームゲートウェイのユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことを可能とするホームゲートウェイ装置、アクセスサーバ装置及び通信方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明に係る通信方法は、ホームネットワークの外部に位置する第１の通信装置から該ホームネットワーク上の第２の通信装置にアクセスするために、該第１の通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、前記所定のメッセージを受信した前記アクセスサーバ装置は、前記第１の通信装置との間で、該第１の通信装置について、予め定められた認証方法に従って認証手続きを行い、前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージを、前記第２の通信装置がサポートするプロトコルに変換した上で、該ホームネットワークを介して、前記第２の通信装置へ転送することを特徴とする。

6

【００１０】また、本発明に係る通信方法は、ホームネットワークの外部に位置する通信装置から該ホームネットワークにアクセスするために、該通信装置から、該ホームネットワークに設置されたホームゲートウェイ装置に対応するアクセス番号を指定して、該ホームゲートウェイ装置に対応するアクセスサーバ装置へ、所定のメッセージを送信し、前記所定のメッセージを受信した前記アクセスサーバ装置は、前記通信装置との間で、該通信装置について、予め定められた認証方法に従って認証手続きを行い、前記アクセスサーバ装置は、前記認証に成功した場合に、指定された前記アクセス番号に対応するホームネットワークに設置されたホームゲートウェイ装置へ、所定のアクセス網を介して、該所定のメッセージを転送し、予め登録された前記アクセスサーバ装置から前記所定のメッセージを受信した前記ホームゲートウェイ装置は、該所定のメッセージに基づいて選択された該ホームネットワークに関係する情報を含むホームページを、前記アクセスサーバ装置を経由して、前記通信装置に転送することを特徴とする。

【００１１】また、本発明は、登録されたホームネットワークのホームゲートウェイ装置に対するアクセス制御を行うアクセスサーバ装置であって、自装置がアクセス制御を行う対象とする前記ホームゲートウェイ装置にアクセスするために使用すべき第１のアクセス番号と、該ホームゲートウェイ装置の設置されるホームネットワークの外部に位置する第１の通信装置が該ホームゲートウェイ装置または該ホームネットワーク上の第２の通信装置に所定のメッセージを送信する際に自装置へアクセスするために使用すべき第２のアクセス番号と、自装置が該第１の通信装置との間で行うべき認証方法とを対応付けて登録した認証テーブルを記憶する手段と、前記ホームネットワークの外部に位置する第１の通信装置から、前記第２のアクセス番号の使用により、前記所定のメッセージを受信する手段と、使用された前記第２のアクセス番号から前記認証テーブルを参照して得られる認証方法に従って、前記第１の通信装置との間で認証手続きを行う手段と、前記認証に成功した場合に、使用された前記第２のアクセス番号から前記認証テーブルを参照して得られる前記第１のアクセス番号を使用し、所定のアクセス網を介して、前記ホームゲートウェイ装置へ、前記所定のメッセージを送信する手段とを備えたことを特徴とする。

【００１２】また、本発明は、ホームネットワークに設

置されるホームゲートウェイ装置であって、前記ホームネットワークと所定のアクセス網との間を中継するための手段と、前記所定のアクセス網を介して通信可能な、自装置に対するアクセス制御を依頼しているアクセスサーバ装置を登録するための手段と、自装置が設置されたホームネットワークの外部からのアクセスを受けた際に、予め登録された前記アクセスサーバ装置からのアクセスのみを許可する手段とを備えたことを特徴とする。

【００１３】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００１４】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００１５】本発明によれば、通信事業者等のサービス事業者側のアクセスサーバ装置にホームネットワーク側のセキュリティ機能（ファイアウォール機能）を受け持たせることで、ホームネットワーク側のホームゲートウェイ装置に過度なセキュリティ機能を実装したり、ホームゲートウェイ装置のユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことが可能になる。

【００１６】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００１７】図１に、本実施形態の通信システムの全体構成例を示す。

【００１８】図１に示されるように、家庭内のホームネットワーク１に、ホームゲートウェイ２と、家電やＡＶやＰＣ等の各種デジタル家電機器（図１の例では、照明器具１１とＶＴＲ１２を例示している）が接続される。ホームネットワーク１は、例えばＩＥＥＥ１３９４やエコーネット等のように、実際には複数のネットワーク技術から構成されていてもよい。また、ホームネットワーク１に接続された機器は、必ずしもインターネットプロトコルに準拠している必要はない。

【００１９】ホームゲートウェイ１は、アクセス網３と接続される。アクセス網３は、例えば、携帯電話のネットワークである。アクセス網３にはアクセスサーバ４が接続されており、アクセスサーバ４がインターネット５と接続されている。

【００２０】なお、アクセス網３上およびまたはホームネットワーク１上をインターネットプロトコル（ＩＰ）に準拠したプロトコルで動作させてもよい（ここでは、説明上、「アクセス網」と「インターネット」とを分けて記述しているが、アクセス網がインターネットプロトコル（ＩＰ）に準拠したプロトコルで動作される場合を排除するものではない）。

【００２１】アクセス網３やアクセスサーバ４はどのようなサービス事業者の管理に属するかについては、種々のバリエーションがある。例えば、アクセス網３とアクセスサーバ４の両方が、携帯電話等の通信事業者の管理に属する（この場合、通信事業者は、ＩＳＰサービスも提供していることになる）。また、例えば、アクセス網３が携帯電話等の通信事業者の管理に属し、アクセスサーバ４がＩＳＰ事業者の管理に属する。また、その他の形態も可能である。

【００２２】ホームゲートウェイ２は、ホームネットワーク１とアクセス網３との間をつなぐ装置である。ホームゲートウェイ２は、家庭内のホームネットワーク１に接続された各種機器（例えば、照明１１やＶＴＲ１２）を家庭外から制御したり、家庭内のＡＶコンテンツ（例えば、ＶＴＲ１２に録画されたＡＶコンテンツ）をアクセス網３を通して家庭外に送信したり、といった種々の機能を実現する。

【００２３】なお、ホームネットワーク１の外部にいる装置（例えば、インターネット５に接続された装置）とホームネットワーク１上の装置とが通信を行う際に、少なくとも、ホームネットワーク１の外部にいる装置とホームゲートウェイ２との間、ホームネットワーク１の外部にいる装置とアクセスサーバ４との間、アクセスサーバ４とホームゲートウェイ２との間のいずれかにおいては、パケット通信を、暗号化や電子署名などを施して行うと好ましい。

【００２４】図２に、ホームゲートウェイ２の内部構成例を示す。

【００２５】図２に示されるように、ホームゲートウェイ２は、ホームネットワーク・インタフェース（ホームネットワークＩ／Ｆ）２１、ホームネット自動構成認識部２２、ホームネット制御ページ作成部２３、ホームネット制御ページ送信部２４、アクセスサーバプロトコル処理部２５、アクセス網インタフェース（アクセス網Ｉ／Ｆ）２６、プロトコル変換及びホームネット制御部２７、高速ＡＶ／ＭＰＥＧ４変換部２８を備えている。

【００２６】本ホームゲートウェイ２では、ホームネットワークＩ／Ｆ２１を介して接続されているホームネット自動構成認識部２２が、ホームネットワーク１に接続された機器を自動的に検出する。例えば、ホームネットワーク１がＩＥＥＥ１３９４であれば、ＩＥＥＥ１２１２レジスタの読み込みや、ＡＶ／Ｃコマンドの発行、ＨＡＶｉレジストリ処理等によって、自動構成認識を行なう。

【００２７】この自動構成認識の結果を、「ホームページ」の形で制御画面に変換するのが、ホームネット制御ページ作成部２３である。この「ホームページ」には、

例えば図３に示すような形で、ホームネットワーク１に接続された家電機器の制御ページが生成される。

【００２８】この「ホームページ」の作成は自動的に行われる。このために、例えば、ホームネット制御ページ作成部２３内に各機器に関するひな形の制御画面をあらかじめ有し、自動構成認識の結果を反映して、このひな形画面を組み合わせたり、各機器から送られてくる制御画面を組み合わせる等して、この「ホームページ」を作成すればよい。

【００２９】生成された家電制御のためのホームページを、インターネット５側からの要求に従って送出するのが、ホームネット制御ページ送信部２４である。ホームネット制御ページ送信部２４は、アクセス網Ｉ／Ｆ３を経由して到着した、ホームゲートウェイ２に対するホームネット制御画面の送出要求メッセージを、アクセスサーバプロトコル処理部２５にて判別し、当該要求をしたインターネット５側の装置（図示せず）に対して、ホームネット制御ページを送出する。

【００３０】上記インターネット５側の装置は、この制御画面を通して、ホームネットワーク１に接続された家電機器の制御要求を行なう。該装置からの制御要求メッセージを受信して、具体的な制御を処理するのが、プロトコル変換及びホームネット制御部２７である。プロトコル変換及びホームネット制御部２７は、この制御要求メッセージを、ホームネットワーク１のプロトコルコマンド（例えばＩＥＥＥ１３９４に接続された装置に対するＡＶ機器への制御要求であれば、ＡＶ／Ｃコマンド）に変換して、これをホームネットワークＩ／Ｆ２１を通して該当機器に送信する。

【００３１】例えば、この要求がホームネットワーク１に接続されたＡＶ機器（例えば、ＶＴＲ１２）に対する「ＡＶデータ再生」要求であったとすると、ホームゲートウェイ２は、該当ＡＶ機器からＡＶデータを受信し、該ＡＶデータを（ホームネットワーク１と比較して送信帯域等に制限がある）アクセス網３に適合させるための符号変換処理（例えばＭＰＥＧ２からＭＰＥＧ４への変換処理）を、高速ＡＶ／ＭＰＥＧ４変換部２８にて行なって、アクセス網Ｉ／Ｆ３を経由して、アクセス網３／インターネット５に対して送出する。

【００３２】図４に、アクセスサーバ４の内部構成例を示す。

【００３３】図４に示されるように、アクセスサーバ４は、アクセス網インタフェース（アクセス網Ｉ／Ｆ）３１、ホームゲートウェイプロトコル処理部３２、第１のファイアウォール処理部（ファイアウォール処理部Ａ）３３、ホームゲートウェイ制御ページ送信部３４、インターネット・インタフェース（インターネットＩ／Ｆ）３５、第２のファイアウォール処理部（ファイアウォール処理部Ｂ）３６を備えている。なお、後述するように、家電機器データベース３７を備えてもよい。

【００３４】なお、本実施形態では、ファイアウォール処理部ＡはＨＴＴＰを処理する機能を含み、ファイアウォール処理部ＢはＡＶデータ転送のためのプロトコルを処理する機能を含むものとする。なお、その代わりに、例えば、ファイアウォール処理部Ａはインターネット５からアクセス網３／ホームネットワーク１方向へのパケットを処理する機能を含み、ファイアウォール処理部Ｂはホームネットワーク１／アクセス網３からインターネット５方向へのパケットを処理する機能を含むように構成するなど、種々の方法がある。もちろん、ファイアウォール処理部を二つに分けずに構成してもよい。

【００３５】アクセスサーバ４のインターネット５側には、ホームゲートウェイ制御ページ送信部３４があり、ホームゲートウェイ制御ページ送信部３４が、実際の（特定の）ホームゲートウェイ２のために、（該特定の）ホームゲートウェイの制御ページの送信を代行する。また、アクセス網３側には、ホームゲートウェイプロトコル処理部３２があり、ホームゲートウェイ２とアクセスサーバ４との間に定義された後述するようなプロトコル処理を行なう。

【００３６】なお、このアクセスサーバ４は、同時に複数のホームゲートウェイに対してサービスを提供することが可能であり、後述するようなサービスを、並行して、同時にいくつも提供することが可能である（すなわち、同時に複数のホームゲートウェイのプロキシとなることができる）。

【００３７】次に、例えばユーザがこのホームゲートウェイを購入した際などに、ユーザが、このホームゲートウェイに対するプロキシサービスの利用を、該サービスを提供するサービス事業者（例えば、携帯電話等の通信事業者）へ申し込む場合について説明する。

【００３８】本実施形態の場合、ホームゲートウェイ２に対するプロキシサービスの利用をサービス事業者に対して登録する。サービス事業者は、アクセスサーバ４を用意する。そのユーザ自身を含めた一般ユーザは、このアクセスサーバ４を介して、このホームゲートウェイ２にアクセスするようなアーキテクチャとなる（すなわち、アクセスサーバ４が、このホームゲートウェイ２のプロキシとなる）。これは、そのホームゲートウェイ２へのアクセスを、一旦、そのサービス事業者のアクセスサーバ４を経由させることで、いわゆる「ファイアウォール処理」等のセキュリティ機能をサービス事業者側によって提供することとし、ホームゲートウェイ４側に、過度なセキュリティ機能を用意しなくとも、ハッカーなどの悪意ユーザの進入防止に代表されるようなセキュリティ処理を達成させることが可能となる。

【００３９】図５に、この場合のシーケンスの一例を示す。

【００４０】まず、ユーザは、ホームゲートウェイ購入時あるいはそのホームゲートウェイの使用をサービス事

業者に申告（申し込み）するときなどの所定のタイミングで、そのユーザを認証するための認証方法（アクセスサーバとそのユーザとの間を認証するための認証方法）を登録する（ステップＳ１）。例えば、この個人認証方法としては、パスワードによる認証や、指紋照合や角膜照合、予め決められた鍵や署名の交換、特定の携帯電話やパソコンからのアクセスに限定してそのソースアドレス（電話番号等）から判定する方法等、種々のものが考えられる。

【００４１】次に、サービス事業者は、そのユーザへ、そのホームゲートウェイ２に対するアクセスのために使用すべきアクセス番号を与える（ステップＳ２）。例えば、そのユーザが、自分のホームゲートウェイ２へのアクセスを携帯電話から行なうことを希望したとすると、サービス事業者は、そのホームゲートウェイ２に対するアクセスのために使用すべきアクセス番号として、例えば、０９０－１２３４－ＸＸＸＸを与える。以降、ユーザは、このアクセス番号０９０－１２３４－ＸＸＸＸを入力すれば、このホームゲートウェイ２へのアクセスを試みることが可能となる（まず認証から行なうことになる）。

【００４２】なお、ステップＳ１やＳ２での情報のやり取りは、アクセス網３を介して行ってもよいし、アクセス網３以外の通信網を介して行ってもよいし、記録媒体を介して行ってもよい。

【００４３】さて、上記のように申告された内容が、アクセスサーバ４内のファイアウォール処理部Ａ内の認証テーブルに登録される（ステップＳ３）。

【００４４】ここで、認証テーブルの例を図６に示す。図６に例示されるように、この認証テーブルは、アクセス番号、個人認証方式、アクセス番号との通信方法、認証内容、プロキシサービスの対象となる実際のホームゲートウェイのアドレス（アクセス番号）などが記載されている。

【００４５】この認証テーブルを参照することによって、

・どのアクセス番号にアクセスしてきたユーザについては、該ユーザが申し込みをした（あるいは予め登録された）本人であるかを、どのような個人認証方式で認証するか、およびその具体的な認証の手続きに関する認証内容、

・インターネット５側のユーザと、このアクセスサーバ４のアクセス番号との通信方法、

・プロキシサービスの対象となる実際のホームゲートウェイ２へのアクセスはどのように行なえばよいか、等を知ることができる。

【００４６】なお、インターネット５側のユーザとこのアクセスサーバ４のアクセス番号との通信方法には、ＳＳＬ、Ｓ－ＨＴＭＬ等のセキュリティを確保するためのプロトコルを使用するのが好ましい。パケット通信を暗

号化や電子署名などを施して行うことによって、ユーザとアクセスサーバ４との間の通信の秘密を保つことが可能となる。

【００４７】また、ホームゲートウェイ２側には、このアクセスサーバ４がいわゆる「プロキシサーバ」として登録される（ステップＳ４）。これは、ユーザが手動で行なってもよいし、サービス事業者あるいは販売店舗などが代行して設定してもよいし、ＩＣカードやメモリカードなどに記憶させて、後でユーザがこのカードをホームゲートウェイ２に装着するなどして登録する方法により行なう等、様々な方法が考えられる。

【００４８】このホームゲートウェイ２は、インターネット５側からあるいはアクセス網３側からあるいはホームネットワーク１の外部からのアクセスについて、プロキシサーバとして登録されたアクセスサーバ４以外からのアクセスは一切受け付けないようにする。このようにすることで、ホームゲートウェイ２のセキュリティの設定は著しく簡単なものとなる。また、このホームゲートウェイ２とアクセスサーバ４との間の通信は、例えばＩＰＳｅｃ等のセキュリティプロトコルによって、成りすまし等の攻撃を未然に防ぐように設定される。または、アクセスサーバ４とホームゲートウェイ２との間は、専用線接続にて接続する。このようにすることで、ホームゲートウェイ２へのアクセスは、すべて（該ホームゲートウェイ２のプロキシとなっている）アクセスサーバ４を経由して行なわなければならないようになるため、該アクセスサーバ４のセキュリティが万全であれば、ホームゲートウェイ２あるいはホームネットワーク１に対する悪意ユーザからの進入等を未然に防ぐことが可能となる。

【００４９】次に、インターネット５上の装置がアクセスサーバ４／アクセス網３／ホームゲートウェイ２を介して、ホームネットワーク１上の家電機器と通信する際のシーケンスについて説明する。

【００５０】ここでは、具体例として、インターネット５に接続された携帯電話（例えばインターネットサービス利用機能を有する携帯電話等）からホームゲートウェイ２を介して家電機器を遠隔操作する場合について説明する。

【００５１】図７および図８に、この場合のシーケンスの一例を示す。

【００５２】ホームゲートウェイ２は、所定のタイミングで、ホームネット自動構成認識部２２により、ホームネットワーク１側に対して構成問合せメッセージを送信し（ステップＳ１１）、家電機器やホームネット１上のディレクトリサーバ（図示せず）などからの構成応答メッセージを受信し（ステップＳ１２）、該構成応答メッセージに基づいて図３に例示するようなホームネットの制御ページを作成する（ステップＳ１３）。

【００５３】なお、ステップＳ１３において、予めホー

い家電機器が検出さ
ビス、サブユニット
では制御ページが作
合にはホームゲート
い合わせることによっ
る情報を取得できる

シーケンスの一例を

ヽ４は、例えば、最新
情報などの詳細情
家電機器データベー
ちろん，最新の家電
部または一部の家電機
ってもよい）。図１１
を示す。
２は、ステップＳ１３
２に登録されていない
ームゲートウェイ１
ハない家電機器を示す
サービスの種別、あ
お問い合わせメッセー
る（ステップＳ１０

セージを受信したアク
機器（例えば、機器、
）について家電機器デ
ノブＳ１０２）。
ーバ４は、問い合わせ
種別に、適切なデータ
制御画面等）を含む応
１０３）。
を受信したホームゲー
器に関する詳細情報や
ホームネット制御ペー
１０５）。
ウェイ２は、取得した
制御画面等のデータを、
制御部２７に追加登録
ップＳ１０４）。
ワーク１上の家電機器
携帯電話（図示せず）か
、アクセス要求メッセ
に送出する（ステップＳ
定められたアクセス番号
ＸＸＸ）に対してアク
スサーバ４に対してアク
とはない（むしろ、所望
てアクセスしようとして

【００６２】アクセス要求メッセージを受けたアクセスサーバ４は、要求されたアクセス番号をもとに、認証テーブルを参照して、認証方式を確認し（ステップＳ２２）、これに合わせて送信ユーザ（携帯電話）に対して認証のチャレンジを行なう（ステップＳ２３）。

【００６３】この認証のチャレンジを受けた携帯電話は、適切なレスポンス（例えばパスワード入力や指紋の入力など）をアクセスサーバに返す（ステップＳ２４）。

【００６４】このレスポンスを受けたアクセスサーバ４は、認証内容の確認を行なう（ステップＳ２５）。

【００６５】もし、本人であることの確認がなされたならば、アクセスサーバ４は、認証テーブルを参照して該当するホームゲートウェイ２を調べ、該ホームゲートウェイ２に対して、アクセス網３を通して、初期ページの送信要求を行なう（ステップＳ２６）。

【００６６】送信要求メッセージを受けたホームゲートウェイ２は、アクセス網３を通して、初期ページをアクセスサーバに送信する（ステップＳ２７）。

【００６７】なお、ステップＳ１１～Ｓ１３は、ステップＳ２６とステップＳ２７との間で行ってもよい。

【００６８】アクセスサーバ４は、このようにして取得した初期ページを、自身のホームゲートウェイ制御ページ送信部３４が送信しているがごとく振るまい、携帯電話に対して、これを送信する（ステップＳ２８）。なお、その際、アクセスサーバ４は、ＨＴＭＬからＣ－ＨＴＭＬ（コンパクトＨＴＭＬ；携帯電話で使われるＷｅｂページの記述言語の一種）への変換など、必要なホームページの記述形式の変換を行なってもよい。また、ホームゲートウェイ２が持つ初期ページを予めキャッシュしておいてもよい。

【００６９】さて、ここで、携帯電話が「ホームネット制御ページ」の送信要求メッセージを送ってきたとする（ステップＳ２９）。アクセスサーバ４のファイアウォール処理部Ａは、このセキュリティ確認を行ない（ステップＳ３０）、確認が取れた（予め登録されたユーザからの要求であると確認された）場合、ホームネット制御ページ要求メッセージをホームゲートウェイ２に対して送信する（ステップＳ３１）。

【００７０】ホームゲートウェイ２は、ホームネット制御ページをアクセスサーバ４に対して送信する（ステップＳ３２）。

【００７１】この制御ページは、アクセスサーバ４のホームゲートウェイ制御ページ送信部３４を介して、携帯電話に送られる（ステップＳ３３）。なお、携帯電話は、アクセスサーバ４からこの制御ページが送られてきた、という認識を持っていてもよい。

【００７２】ここで、携帯電話にて、例えば制御対象の装置としてＶＴＲが指定されたとすると、その制御コマンド（例えばホームネット制御ページの適切なボタンを

15

押す動作）がアクセスサーバ４に伝えられる（ステップＳ３４）。

【００７３】アクセスサーバ４は、再びセキュリティの確認を行ない（ステップＳ３５）、確認が取れた場合は、ホームゲートウェイ２に対して、ＶＴＲ制御のためのコマンド（例えばホームネット制御ページの適切なボタンを押す動作）を送信する（ステップＳ３６）。

【００７４】ホームゲートウェイ２では、受け取ったコマンドをプロトコル変換及びホームネット制御部２７においてホームネットワークプロトコルに準拠した制御コマンドに変換して（ステップＳ３７）、これをＶＴＲなどの家電機器に送信する（ステップＳ３８，Ｓ３９）。その際、必要な場合は、ホームネットワーク上での帯域確保等も伴うことがある。

【００７５】さて、この結果、家電機器から例えば高速映像信号などがホームゲートウェイ２に対して流れてくる（ステップＳ４０）。

【００７６】ホームゲートウェイ２の高速ＡＶ／ＭＰＥＧ４変換部２８は、この高速映像信号をＭＰＥＧ４信号などに変換する（ステップＳ４１）。このようにすることにより、アクセス網に適した形（例えば、限定された帯域に合わせて、映像の高圧縮が行なわれる）でデータ送信を行なうことができるようになる。

【００７７】このように変換されたＭＰＥＧ４映像は、アクセスサーバ４に対して送られる（ステップＳ４２）。

【００７８】アクセスサーバ４では、ファイアウォール処理部Ｂにおいて、必要なファイアウォール処理（ＮＡＴ処理やＩＰマスカレード処理）を施し（ステップＳ４３）、このＭＰＥＧ４映像は、インターネット５を介して携帯電話に届けられる（ステップＳ４４）。

【００７９】このようにして、携帯電話のユーザは、携帯電話／インターネットを通して自宅の家電を制御したり、自宅内のＡＶコンテンツを携帯電話にて閲覧したりといったことが可能となる。

【００８０】なお、上記では、携帯電話からアクセスサーバ４までの接続が一旦インターネット５を経由するものとして説明したが、例えばインターネットサービスを提供する通信事業者の通信網（図１のアクセス網３であってもよい）を経由して携帯電話がアクセスサーバ４に接続する（すなわちインターネット５を経由せずに接続する）ような場合も同様である。

【００８１】これまでは、インターネット５側からホームネット１側へのアクセスについての例であった。次に、ホームネット１側からインターネット５側へのアクセスの例について説明する。

【００８２】図９に、この場合のシーケンスの一例を示す。

【００８３】ここでは、ホームネットワーク１上に家電機器としてパソコンが接続されたと仮定して（図示せず）、このパソコンからインターネット５上のＷＷＷサーバ（図示せず）へのアクセスが行なわれた場合を例にとって説明する。

16

【００８４】まず、前述のようにパソコン上には、アクセスサーバ４がプロキシサーバとして登録されている（ステップＳ５１）。

【００８５】パソコン上からインターネット５上のＷＷＷサーバへのアクセス要求があった場合、プロキシサーバであるアクセスサーバ４に対して、そのアクセス要求メッセージが送られる（ステップＳ５２）。

【００８６】アクセスサーバ４では、ファイアウォール処理部Ａによってプロキシ処理が行なわれ（ステップＳ５４）、実際のＷＷＷサーバに対してアクセス要求メッセージが転送される。ただし、このアクセスサーバ４が要求したものとして転送される。

【００８７】ＷＷＷサーバは、これに対する応答メッセージを送信し、これをアクセスサーバ４のファイアウォール処理部Ａが受信する（ステップＳ５５）。

【００８８】アクセスサーバ４のファイアウォール処理部Ａは、該応答メッセージについて、プロキシサーバ処理（例えばＮＡＴやＩＰマスカレード処理、アプリケーションゲートウェイ処理など）を行ない（ステップＳ５６）、実際の応答メッセージをパソコンに転送する（ステップＳ５７）。

【００８９】このやり取りが、任意のＷＷＷサーバに対するアクセスに対して行なわれる。

【００９０】なお、図９上では、パソコンからアクセスサーバ４に対して直接パケットが飛んでいるように記述されているが、もちろんホームゲートウェイ２にて一旦パケットが終端されてもよい。すなわち、ホームゲートウェイ２において、アプリケーションゲートウェイ処理やＮＡＴ処理、ＩＰマスカレード処理などの処理がなされて、アクセスサーバ４から見るとホームゲートウェイ２のみと通信しているように見えるようなアーキテクチャとなっていてもよい。

【００９１】この場合は、パソコンに登録されているプロキシサーバがホームゲートウェイであってもよい。

【００９２】また、上記では、ＷＷＷサーバはインターネット上に存在するものとして説明したが、例えばインターネットサービスを提供する通信事業者の通信網（図１のアクセス網３であってもよい）内に存在するＷＷＷサーバにアクセスする（すなわちインターネット５を経由せずにアクセスする）ような場合も同様である。

【００９３】また、サービス事業者によって提供される（アクセスサーバ４による）プロキシサービスを利用するか、ユーザが従来のようにネットワーク管理者になってホームゲートウェイ２に対して直接必要な設定や作業を行うかを、ユーザ自身が任意に選択できるようにしてもよい。また、それらを併用可能としてもよい。

【００９４】なお、基本的にはアクセスサーバが提供す

17

るプロキシサービスを利用するものとした上で、さらにホームゲートウェイ２にネットワーク管理者に要求される知識を有さずとも簡易な手続きで認証のための設定ができる機能を付与し、限られた装置またはユーザのみ外部（インターネット）から直接ホームゲートウェイ２にアクセスできるようにしてもよい。例えば、ホームゲートウェイ２にパスワード等を登録しておき、外部からのアクセス時にユーザが正しいパスワード等を携帯電話等の端末装置へ入力し（あるいは携帯端末等にパスワード等を登録しておきあるいは登録されており）、正しいパスワード等を返答してきた携帯端末のみホームゲートウェイ２がアクセスを許可するようにする方法など、種々の方法がある。

【００９５】なお、以上の各機能は、ソフトウェアとしても実現可能である。また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【００９６】なお、本実施形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、本実施形態内において、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、各実施形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

【００９７】従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【００９８】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００９９】

【発明の効果】本発明によれば、通信事業者等のサービス事業者側のアクセスサーバ装置にホームネットワーク側のセキュリティ機能（ファイアウォール機能）を受け持たせることで、ホームネットワーク側のホームゲートウェイ装置に過度なセキュリティ機能を実装したり、ホームゲートウェイ装置のユーザに専門的な設定、管理などを要求したりすることなしに、ホームネットワークに対する悪意ユーザからの攻撃を未然に防ぐことが可能になる。

18

【図面の簡単な説明】

【図１】本発明の一実施形態に係る通信システムの全体構成例を示す図

【図２】同実施形態に係るホームゲートウェイの内部構成例を示す図

【図３】同実施形態に家電機器の制御ページの一例を示す図

【図４】同実施形態に係るアクセスサーバの内部構成例を示す図

【図５】同実施形態に係る登録のためのシーケンスの一例を示す図

【図６】同実施形態に係る認証テーブルの一例を示す図

【図７】同実施形態に係る外部からホームネットワーク側へのアクセスの際のシーケンスの一例を示す図

【図８】同実施形態に係る外部からホームネットワーク側へのアクセスの際のシーケンスの一例を示す図７の続きの図

【図９】同実施形態に係るホームネットワーク側から外部へのアクセスの際のシーケンスの一例を示す図

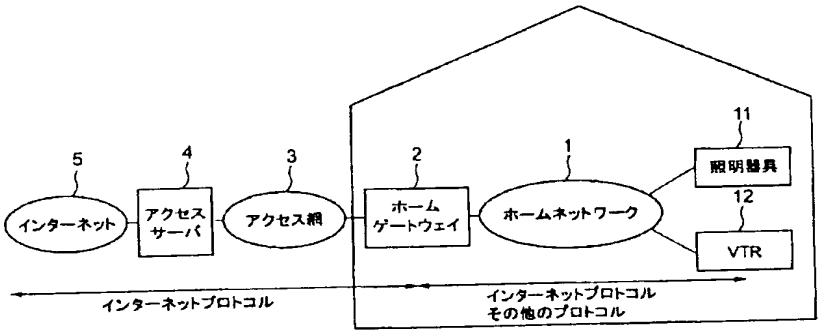
【図１０】同実施形態に係るホームネット制御ページの際のシーケンスの一例を示す図

【図１１】同実施形態に係る家電機器データベースの一例を示す図

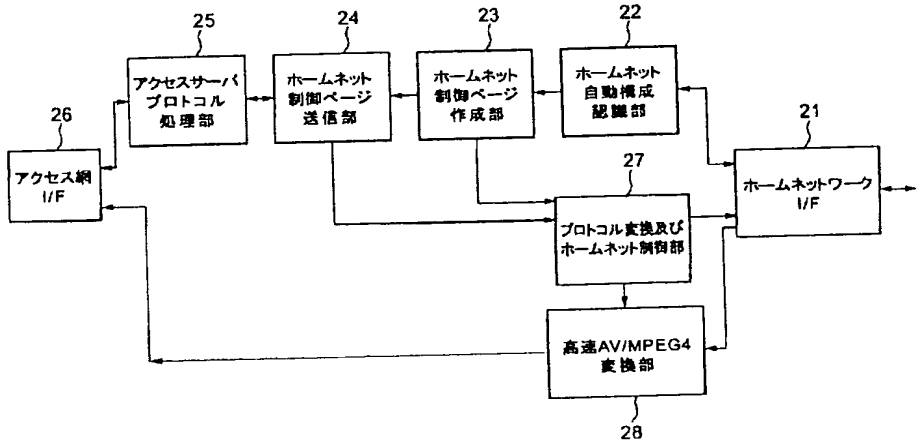
【符号の説明】

１…ホームネットワーク
２…ホームゲートウェイ
３…アクセス網
４…アクセスサーバ
５…インターネット
１１…照明器具
１２…ＶＴＲ
２１…ホームネットワーク・インタフェース
２２…ホームネット自動構成認識部
２３…ホームネット制御ページ作成部
２４…ホームネット制御ページ送信部
２５…アクセスサーバプロトコル処理部
２６，３１…アクセス網インタフェース
２７…プロトコル変換及びホームネット制御部
２８…高速ＡＶ／ＭＰＥＧ４変換部
３２…ホームゲートウェイプロトコル処理部
３３…第１のファイアウォール処理部
３４…ホームゲートウェイ制御ページ送信部
３５…インターネット・インタフェース
３６…第２のファイアウォール処理部
３７…家電機器データベース

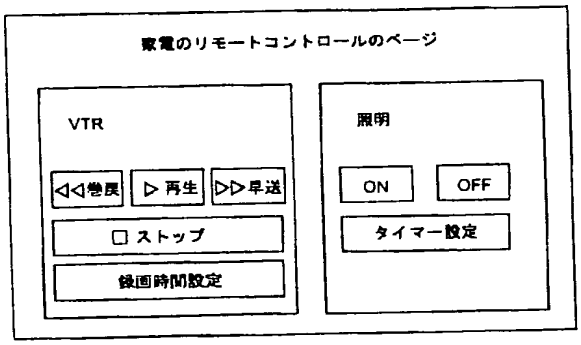
【図１】


5
4
3
2
1
11
12
インターネット
アクセス サーバ
アクセス網
ホーム ゲートウェイ
ホームネットワーク
照明器具
VTR
インターネットプロトコル
インターネットプロトコル
その他のプロトコル

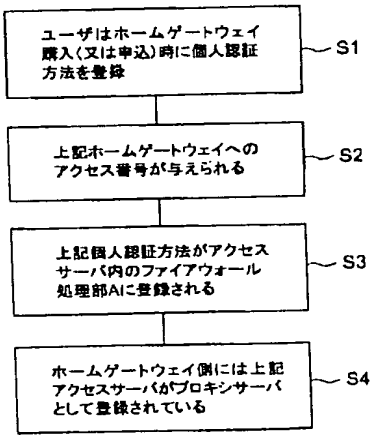
【図２】


25
24
23
22
26
21
27
アクセスサーバ プロトコル 処理部
ホームネット 制御ページ 送信部
ホームネット 制御ページ 作成部
ホームネット 自動構成 認識部
アクセス網 I/F
ホームネットワーク I/F
プロトコル変換及び ホームネット制御部
高速AV/MPEG4 変換部
28

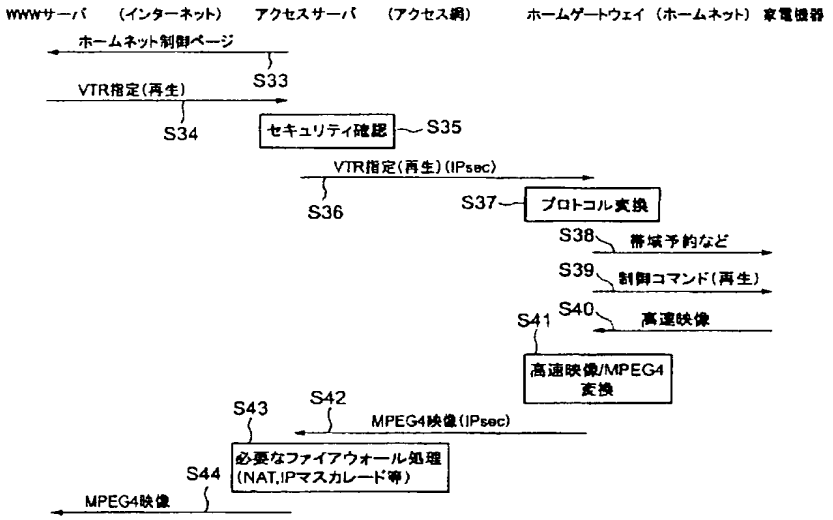
【図３】


家電のリモートコントロールのページ
VTR
巻戻
再生
早送
ストップ
録画時間設定
照明
ON
OFF
タイマー設定

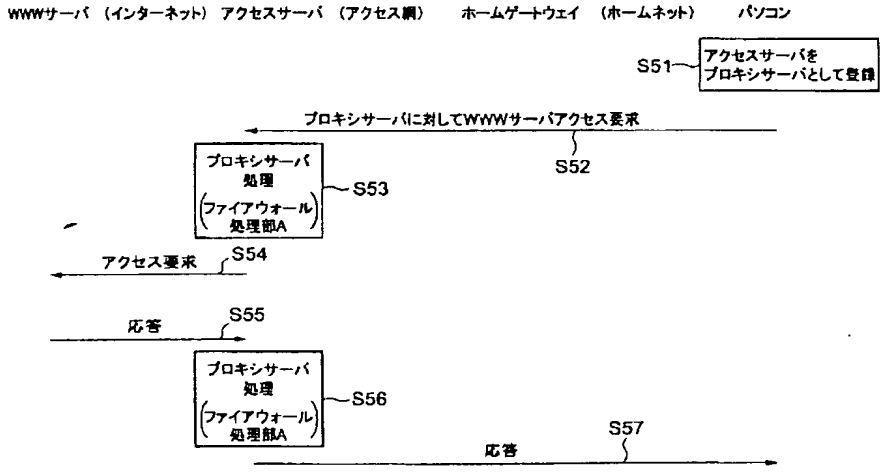
【図５】


ユーザはホームゲートウェイ 購入(又は申込)時に個人認証 方法を登録
S1
上記ホームゲートウェイへの アクセス番号が与えられる
S2
上記個人認証方法がアクセス サーバ内のファイアウォール 処理部Aiに登録される
S3
ホームゲートウェイ側には上記 アクセスサーバがプロキシサーバ として登録されている
S4

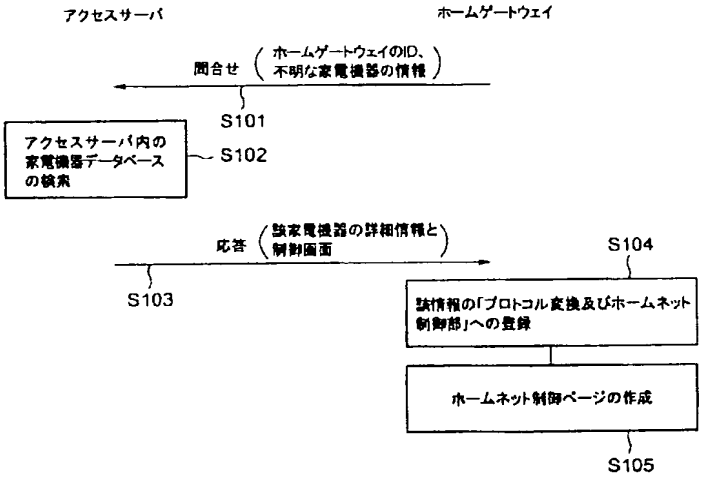
【図８】


WWWサーバ
（インターネット）
アクセスサーバ
（アクセス網）
ホームゲートウェイ（ホームネット）
家電機器
ホームネット制御ページ
S33
VTR指定(再生)
S34
セキュリティ確認
S35
VTR指定(再生)(IPsec)
S36
S37
プロトコル変換
S38
帯域予約など
S39
制御コマンド(再生)
S40
高速映像
S41
高速映像/MPEG4
変換
S43
S42
MPEG4映像(IPsec)
必要なファイアウォール処理
(NAT,IPマスカレード等)
S44
MPEG4映像

【図９】


WWWサーバ
（インターネット）
アクセスサーバ
（アクセス網）
ホームゲートウェイ
（ホームネット）
パソコン
S51
アクセスサーバを
プロキシサーバとして登録
プロキシサーバに対してWWWサーバアクセス要求
S52
プロキシサーバ
処理
(ファイアウォール
処理部A)
S53
アクセス要求
S54
応答
S55
プロキシサーバ
処理
(ファイアウォール
処理部A)
S56
S57
応答

【図１０】



【図１１】

ネットワーク種別	サービス/サブユニット名	属性情報	制御画面
IEEE1394	ホームサーバ	（XMLデータ形式）	（XMLデータ形式）
⋮	⋮	⋮	⋮
エコーネット	自動そうじ機	（XMLデータ形式）	（XMLデータ形式）
⋮	⋮	⋮	⋮

（これらがホームゲートウェイの機種別に用意される）